UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/510,498	05/04/2005	Jesus Angel de Gregorio Rodriguez	4020-3	1556

23117   7590   02/07/2008

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
ZEWARI, SAYED T

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
02/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/510,498	GREGORIO RODRIGUEZ ET AL.
Office Action Summary	Examiner	Art Unit	
	Sayed T. Zewari	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 November 2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-25_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-25_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

1.   The Art Unit location of your application in the USPTO has changed. To aid in correlating any papers for this application, all further correspondence regarding this application should be directed to Art Unit 2617.

Response to Amendment

2.   Applicant's arguments filed on 11/23/2007 have been fully considered but they are not persuasive.

3.   Applicant argument stating that

> *So in Haverinen et al., the IP address is allocated to the mobile terminal prior to authenticating the mobile terminal with the underlying mobile network. Claim 1, in contrast, recites that the IP address is sent to the wireless terminal after a successful authentication. Accordingly, independent claim 1 is distinguishable over Haverinen et al.*

is not persuasive. Haverinen does not disclose allocating IP address prior to authentication. In fact, it is common knowledge that authentication always takes place before any device is connected to a network. However, applicant is still referred to Svensson (US 2003/0120920) and figure 2 and section [0025] and [0026] where this limitation is disclosed.

DETAILED ACTION

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5.   Claims 1-5, 7-13, 15-22, 24, and 25 are rejected under 35 U.S.C. 102(b) as being

anticipated by Haverinen et al. (2002/0,012,433).

With respect to claim 1, Haverinen discloses a method in a telecommunication

system for allowing a SIM-based authentication to users of a wireless local area

network who are subscribers of a public land mobile network **(See Haverinen's**

abstract, see figure 7 & 8, sections [0242] - [0244], [0247], [0249] - [0251], [0255] -

[0258]), the method comprising:

(a) a wireless terminal accessing the wireless local area network through an

accessible Access Point **(See Haverinen's abstract, see figure 7 & 8, sections [0242]**

- [0244], [0247], [0249] - [0251], [0255] - [0258]);

(b) discovering an Access Controller interposed between the Access Point and the

public land mobile network from the wireless terminal **(See Haverinen's abstract, see**

figure 7 & 8, sections [0242] - [0244], [0247], [0249] - [0251], [0255] - [0258]);

(c) carrying out a challenge-response authentication procedure between the wireless

terminal and the public land mobile network through the Access Controller **(See**

Haverinen's abstract, section [0018], [0020], [0021], [0022], [0029], [0034], [0109],

[0138], [0170], [0315], see additional information at section [0009] - [0013]), the

wireless terminal provided with a SIM card and adapted for reading data thereof (See

Haverinen's abstract, see figure 7 & 8, sections [0242] - [0244], [0247], [0249] -

[0251], [0255] - [0258]); wherein the challenge-response authentication submissions in

step c) take place before having provided IP connectivity to the user (See Haverinen's

abstract, section [0014] - [0029], [0343]), and are carried:

    - on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless

terminal and the Access Controller (See Haverinen's [0343]); and

    - on an authentication protocol residing at an application layer between the

public land mobile network and the Access Controller (See Haverinen's [0003], [0263]-

[0269]); and the method further comprising:

(d) offering the IP connectivity to the user at the wireless terminal, by sending an

assigned IP address and other network configuration parameters, once said user

has been validly authenticated by the public land mobile network (See Haverinen's

abstract, section [0014] - [0029], [0343]).

    With respect to claim 15, Haverinen discloses an Access Controller in a

telecommunication system that comprises a wireless local area network including at

least one Access Point, a public land mobile network, and at least one wireless terminal

provided with a SIM card and adapted for reading subscriber data thereof (See

Haverinen's abstract, see figure 7 & 8, sections [0242] - [0244], [0247], [0249] -

[0251], [0255] - [0258]), the Access Controller comprising:

a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the

wireless terminal over a PPPoE protocol, the PPPoE server being arranged for

tunneling a challenge-response authentication procedure **(See Haverinen's abstract,**

section [0343], [0018], [0020], [0021], [0022], [0029], [0034], [0109], [0138], [0170],

[0315], see additional information at section [0009] - [0013]); and

an authentication client for communicating with the public land mobile network,

wherein the authentication client is configured to implement an authentication protocol

residing at an application layer, wherein the access Controlller is configured to send an

assigned IP address and other network configuration parameters to the wireless

terminal to provide IP connectivity after the challenge-response authentication

procedure is successfully carried out between the wireless terminal and the public land

mobile network in the telecommunication system. **(See Haverinen's [0003], [0263]-**

[0269]).

With respect to claim 25, Haverinen discloses a telecommunication system

comprising a wireless local area network that includes at least one Access Point, a

public land mobile network, at least one wireless terminal provided with a SIM card and

adapted for reading subscriber data thereof, and the Access Controller in claims 15 for

allowing SIM-based subscriber authentication to users of the wireless local area

network who are subscribers of the public land mobile network **(See Haverinen's**

abstract, see figure 7 & 8, sections [0242] - [0244], [0247], [0249] - [0251], [0255] -

[0258]).

With respect to claim 2, Haverinen discloses a method wherein the step (b) includes establishing a Point-to-Point Protocol session between a Point-to-Point over Ethernet (PPoE) Protocol client in the wireless terminal and a Point-to-Point over Ethernet (PPoE) Protocol server in the Access Controller **(See Haverinen's abstract, see figure 7 & 8, sections [0242] - [0244], [0247], [0249] - [0251], [0255] - [0258])**.

With respect to claim 3, Haverinen discloses a method wherein the step (c) **(See Haverinen's abstract, section [0018], [0020], [0021], [0022], [0029], [0034], [0109], [0138], [0170], [0315], see additional information at section [0009] - [0013])** includes:

(c1) sending a user identifier from the wireless terminal to the public land mobile network through the Access Controller **(See Haverinen's see figure 9, section [0263]-[0279])**;

(c2) receiving an authentication challenge at the wireless terminal from the public land mobile network via the Access Controller **(See Haverinen's see figure 9, section [0263]-[0279])**;

(c3) deriving encryption key and authentication response at the wireless terminal from the received authentication challenge **(See Haverinen's see figure 9, section [0263]-[0279])**;

(c4) sending the authentication response from the wireless terminal to the public land mobile network through the Access Controller **(See Haverinen's see figure 9, section [0263]-[0279])**;

(c5) receiving at the Access Controller an encryption key from the public land

mobile network **(See Haverinen's see figure 9, section [0263]-[0279])**; and

(c6) extracting the encryption key received for further encryption of

communication path with the wireless terminal **(See Haverinen's see figure 9, section**

[0263]-[0279]).

With respect to claim 4, Haverinen discloses a method further comprising shifting

authentication information received on top of the Point-to-Point layer 2 protocol upwards

to the authentication protocol residing at the application layer for submissions toward

the public land mobile network **(See Haverinen's see figure 9, section [0285]-[0305])**.

With respect to claim 5, Haverinen discloses a method further comprising the

step of shifting authentication information received on the authentication protocol

residing at application layer downwards on top of the Point-to-Point layer 2 protocol for

submissions toward the wireless terminal **(See Haverinen's see figure 9, section**

[0285]-[0305]).

With respect to claim 7, Haverinen discloses a method wherein the step (d)

includes a previous step of requesting the assigned IP address from a Dynamic Host

Configuration Protocol server **(See Haverinen's see figure 9, section [0263]-[0279])**.

With respect to claim 8, Haverinen discloses a method wherein the

communication between the Access Controller and the public land mobile network goes

through an Authentication Gateway of said public land mobile network **(See**

Haverinen's see figure 9, section [0263]-[0279]).

With respect to claim 9, Haverinen discloses a method wherein the communication between the Access Controller and an Authentication Gateway of the public land mobile network goes through an Authentication Server of the wireless local area network in charge of authenticating local users of said wireless local area network who are not mobile subscribers **(See Haverinen's see figure 9, section [0263]-[0279])**.

With respect to claim 10, Haverinen discloses a method wherein the user identifier in step (c) comprises a Network Access Identifier **(See Haverinen's see figure 16, section [0346], [0371])**.

With respect to claim 11, Haverinen discloses a method wherein the user identifier in step c) comprises an International Mobile Subscriber Identity **(See Haverinen's see figure 9, section [0263]-[0279], see additional information at section [0242], [0244], [0247], [0250], [0255], [0258])**.

With respect to claim 12, Haverinen discloses a method wherein the authentication protocol residing at the application layer in step (c) is an Extensible Authentication Protocol **(See Haverinen's see figure 16, section [0342]-[0347], [0348]-[0350])**.

With respect to claim 13, Haverinen discloses a method wherein this Extensible Authentication Protocol is transported over a RADIUS protocol **(See Haverinen's see figure 16, section [0342]-[0347], [0348]-[0350] and [0323])**.

With respect to claim 16, Haverinen discloses an Access Controller wherein

the authentication cline is configured to shift information received on top of the

Point-to-Point layer 2 protocol upwards to the authentication protocol residing at the

application layer **(See Haverinen's see figure 9, section [0285]-[0305])**; and

wherein the PPPoE server is configured to shift information received on the

authentication protocol residing at the application layer downwards on top of the Point-

to-Point layer 2 protocol (PPPoE) **(See Haverinen's see figure 9, section [0285]-**

[0305]).

With respect to claim 17, Haverinen discloses an Access Controller wherein the

Access Controller is adapted for requesting an IP address from a Dynamic Host

Configuration Protocol server, after a user has been successfully authenticated by his

public land mobile network **(See Haverinen's see figure 9, section [0263]-[0279])**.

With respect to claim 18, Haverinen discloses an Access Controller wherein the

Access Controller is adapted for communicating with a wireless terminal via an Access

Point **(See Haverinen's abstract, see figure 7 & 8, sections [0242] - [0244], [0247],**

[0249] - [0251], [0255] - [0258]).

With respect to claim 19, Haverinen discloses an Access Controller wherein the

Access Controller is adapted for communicating with the public land mobile network via

an Authentication Gateway **(See Haverinen's see figure 9, section [0263]-[0279])**.

With respect to claim 20, Haverinen discloses an Access Controller wherein the

Access Controller is adapted for communicating with an Authentication Gateway via an

Authentication Server responsible for authenticating local users of the wireless local

area network **(See Haverinen's see figure 9, section [0263]-[0279])**.

With respect to claim 21, Haverinen discloses an Access Controller wherein the authentication protocol residing at the application layer is an Extensible Authentication Protocol **(See Haverinen's see figure 16, section [0342]-[0347], [0348]-[0350])**.

With respect to claim 22, Haverinen discloses an Access Controller wherein the Extensible Authentication Protocol is transported over a RADIUS protocol **(See Haverinen's see figure 16, section [0342]-[0347], [0348]-[0350] and [0323])**.

With respect to claim 24, Haverinen discloses a wireless terminal capable of carrying out a challenge-response authentication procedure, the wireless terminal comprising a client configured to act as a Point- to-Point layer 2 protocol (PPPoE) client, wherein an Extensible Authentication Protocol is carried on top of a Point-to-Point layer 2 protocol **(See Haverinen's see figure 9, section [0285]-[0305])**.

Claim Rejections - 35 USC § 103

6.　The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.　Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Haverinen et al. (2002/0,012,433) in view of Fink et al. (US 7,043,633).

With respect to claim 6, Haverinen discloses a method of establishing at the wireless terminal an encryption path by using the previously derived encryption keys at the Access Controller and wireless terminal. Haverinen does not disclose a symmetric encryption. But Fink et al. discloses this limitation **(See Fink et al. figure 4, col.8 lines 3-20)**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Haverinen and combine it with Fink, thereby providing a system that uses symmetric encryption as disclosed by Fink et al. **(See Fink et al. figure 4, col.8 lines 3-20)**.

8.   Claims 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haverinen et al. (2002/0,012,433) in view of Amin et al. (US 6,854,014).

With respect to claim 14 and 23, Haverinen discloses a method wherein the Extensible Authentication Protocol is used. Haverinen does not disclose the EAP is transported over a Diameter protocol. But Amin et al. discloses this limitation **(See Amin's col.2 lines 3, lines 9-10, lines 66-67, col.3 line 1)**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Haverinen and combine it with Amin, thereby providing a system that uses Diameter protocol, as disclosed by Amin et al. **(See Amin's col.2 lines 3, lines 9-10, lines 66-67, col.3 line 1)**.

Conclusion

9.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

10.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Sayed T. Zewari whose telephone number is 571-272-

6851. The examiner can normally be reached on 8:30-4:30.

11.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Lester G. Kincaid can be reached on 571-272-7922. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

12.   Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sayed T. Zewari

February 1, 2008

LESTER G. KINCAID
SUPERVISORY PRIMARY EXAMINER